BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 103 41 370.7

Anmeldetag: 8. September 2003

Anmelder/Inhaber: SimonsVoss Technologies AG,
85774 Unterföhring/DE

Bezeichnung: Identifikationssystem

IPC: G 07 C 9/00

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 14. September 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

A 9161
03/00
EDV-L

SimonsVoss Technologies AG
u.Z.: H 2554 DE

08. September 2003

VOSSIUS & PARTNER
PATENTANWÄLTE
SIEBERTSTR. 4
81675 MÜNCHEN

Identifikationssystem

Die vorliegende Erfindung betrifft ein System und ein Verfahren zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu einer Zieleinrichtung. Insbesondere dienen das erfindungsgemäße System und Verfahren zum Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu Zieleinrichtungen wie Schließvorrichtungen, Türzylindern, Möbeln, Schaltschränken, Kraftfahrzeugen, Tresoren, Safes, Geldautomaten, Fahrer- bzw. Bedienberechtigungen, PC Log-ons und/oder das Freischalten von Schußwaffen.

Systeme zur Personenidentifikation sind im Stand der Technik bekannt. So offenbart die DE 199 29 894 A1 eine Vorrichtung sowie ein Verfahren zur daktyloskopischen Personenidentifikation in Gestalt eines elektronischen Schlüssels, wobei sich in diesem ein Sensor zur Detektion von Fingerabdrücken, eine Einrichtung zur vollständigen Bearbeitung des Sensorbildes sowie eine Einrichtung zur Speicherung der Fingerabdrucksmerkmale befindet. Hierbei besteht die Verarbeitung im Schlüssel aus zwei Teilen, der Fingerabdruckerkennung einerseits sowie einer mit bekannter Technik hergestellten kryptologisch gesicherten Schnittstelle zur Außenwelt in Gestalt eines kryptographischen Protokolls.

Die DE 198 48 001 A1 beschreibt ein Verfahren zur Betriebsfreigabe eines Kfz, bei dem aufgrund der Zuführung eines Datenträgers in eine Kfz-seitige Leseeinrichtung, wobei der Datenträger benutzerspezifische Informationen des Inhabers gespeichert hat, welche von der Leseeinrichtung detektiert, einer Kfz-seitigen Recheneinheit zugeführt und mit dort gespeicherten Informationen verglichen werden, wobei vom Benutzer weitere, personenbezogene Informationen von einer Kfz-seitigen Erkennungseinrichtung abgefragt, der Recheneinheit zugeführt und mit Kfz-seitigen gespeicherten, auf die Person des Benutzers bezogenen Informationen verglichen

werden, und aufgrund des Ergebnisses des personenbezogenen Datenvergleichs eine Betriebsfreigabe des Kfz erfolgt oder nicht.

Die DE 101 26 050 A1 schlägt ein Verfahren zur Benutzerfassung eines Kraftfahrzeugs vor, bei dem ein physiologisches Merkmal eines Benutzers ermittelt wird und mit gespeicherten Daten verglichen wird, wodurch sicher gestellt werden soll, dass das Kraftfahrzeug tatsächlich von einem Berechtigten benutzt wird.

Die DE 197 56 428 A1 betrifft ein Fahrzeugsabsicherungsverfahren, bei dem eine auf physiologische Merkmale des Benutzers gerichtete Erfassungseinheit mit einer Vergleichseinheit zusammenwirkt, in der die Merkmale der berechtigten Benutzer gespeichert sind und die für den berechtigten Benutzer ein Freigabesignal zur Inbetriebnahme des Fahrzeugs erteilt. Ist der Benutzer nicht berechtigt, fragt die Vergleichseinheit eine zusätzliche Identifikationsinformation ab, die in einem vom Benutzer getragenen separaten Speicher enthalten ist, wobei die Vergleichseinheit beim Empfang der zusätzlichen Identifikationsinformation ein Sonderfreigabesignal erteilt.

Die DE 198 42 544 A1 betrifft eine Vorrichtung zum Bestimmen der Fahrerberechtigung, mit der mittels einer Biometriedatenerfassung die Biometriedaten eines Benutzers erfasst werden und in einer Auswerteeinheit mit einem Biometrieprofilspeicher auf Übereinstimmung verglichen werden, wobei eine Berechtigungsfreigabe auch dann erfolgt, wenn die Biometriedaten des Benutzers nicht in dem Biometrieprofilspeicher hinterlegt sind, sofern eine Codeerfassung ein mit einem Betriebsmittelcode übereinstimmendes Betriebsmittelsignal erfasst. Mittels eines speziellen Sonderbetriebsmittels können die zum Anlernen, Löschen oder Ändern bzw. Speichern von Biometrieprofilen und Ressourcen vorgesehenen Betriebsarten ausgewählt und entsprechende Vorgänge durchgeführt werden.

Heutige Systeme zur Personenidentifikation weisen vornehmlich tragbare Authentifizierungsmedien wie beispielsweise Schlüssel, Chipkarten oder Transponder auf, die übertragbar sind. Demnach lässt sich mit ihnen der Nutzer nicht eindeutig authentisieren, da jeweils der Nutzer, der im Besitz des

Authentifizierungsmediums ist, als berechtigt erkannt wird. Derartige Authentifizierungsmedien haben den Nachteil, dass sie gestohlen werden können bzw. bei Verlust mißbraucht werden können. Als Alternative bzw. zusätzliche Absicherung kann eine Identifikation über ein geistiges Medium, wie beispielsweise eine PIN (personal identification number) oder ein Passwort erfolgen. Diese Lösung ist ebenfalls als nicht sicher anzusehen, da die relevanten Informationen ausspioniert bzw. ausprobiert oder erraten werden können.

Insbesondere um obige Probleme zu vermeiden, werden biometrische bzw. physiologische Verfahren verwendet, bei denen Personen anhand von personenspezifischen Merkmalen identifiziert werden, indem diese Merkmale detektiert und mit in einem Speicher hinterlegten Referenzmerkmalen verglichen werden. Hierbei befindet sich die Leseeinrichtung bzw. der Scanner in der Regel fest an der zu verwendenden Einrichtung, beispielsweise einer Tür, installiert. Als nachteilig erweist sich hierbei i.a. das Erfordernis einer on-line Verbindung zu einer zentralen Datenbank. Hierbei ruft das Halten der Datenbank bzw. das Speichern der benutzerspezifischen Daten an einem dem Benutzer nicht zugänglichen Ort unter Umständen Nutzerängste, beispielsweise vor Datenmissbrauch, hervor. Ferner verursacht die Verkabelung und Installation einer Vorrichtung zur Durchführung eines biometrischen Verfahrens hohe Kosten und ist demnach wirtschaftlich nur für wenige Anwendungsfälle geeignet. Insbesondere in Fällen, in denen beispielsweise wenige Benutzer auf wenige Vorrichtungen Zugriff haben sollen oder aber wenn eine hohe Zahl an Vorrichtungen vorhanden ist, erweisen sich derartige Vorrichtungen, insbesondere wirtschaftlich und prozesstechnisch, als nachteilig. Auch wirkt sich ein Berechtigungssignal, beispielsweise zur Öffnung einer Tür, im allgemeinen nur als Öffnungssignal auf den Türsummer auf, d.h. eine verriegelte Tür kann nicht geöffnet werden. Weiterhin befindet sich die aufwendige und teuere Lese- bzw. Scaneinrichtung für biometrische Merkmale verfahrensgemäß im Außenbereich, d.h. in einem einer Vielzahl von Personen zugänglichen Bereich. Derartige Einrichtungen unterliegen somit der Gefahr der Beschädigung bzw. Manipulation. Ferner haben Unberechtigte beliebig viel Zeit, um zu versuchen, die Einrichtung zu überlisten (siehe zum Beispiel Zeitschrift „CT“ vom Mai/Juni 2002).

Weiterhin gestaltet sich die Pflege der entsprechenden Datenbank als aufwendig und kostenintensiv, da neue Benutzer umständlich eingelesen werden müssen und die Vergleichsdaten nicht mehr berechtigter Personen umständlich gelöscht werden müssen.

Auch gestaltet sich die Verwendung derartiger Verfahren für den Nutzer häufig als umständlich und aufwendig, da für mehrere, beispielsweise rasch aufeinanderfolgende, Zugriffe, beispielsweise auf ein Kraftfahrzeug, ein mehrfaches Durchführen des Identifikationsverfahrens erforderlich wird. Eine zusätzliche Gültigkeit tragbarer, nicht personenspezifischer Authentifizierungsmedien macht hierbei mögliche Vorteile einer personenabhängigen Identifikation zunichte. Nachteile ergeben sich demnach insbesondere bei Systemen mit einer Vielzahl von berechtigten Benutzern, einer Benutzerhierarchie mit unterschiedlichen Berechtigungsstufen, sowie sich häufig änderten Benutzerzahlen bzw. Strukturen.

Der Erfindung liegt die Aufgabe zugrunde, ein System und Verfahren zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder eins physikalischen Zugangs zu einer Zieleinrichtung bereitzustellen, das die obigen Nachteile überwindet. Ferner ist es Aufgabe der vorliegenden Erfindung ein System und Verfahren bereitzustellen, das kostengünstig ist, zuverlässig arbeitet und benutzerfreundlich zu bedienen ist.

Die Lösung dieser Aufgabe(n) gelingt mit einem System bzw. einem Verfahren entsprechend den unabhängigen Ansprüchen. Die Unteransprüche betreffen bevorzugte Ausführungsformen.

Ein erfindungsgemäßes System zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu einer Zieleinrichtung weist ein tragbares Identmedium auf. Das tragbare Identmedium wiederum weist mindestens einen Biometriesensor, mindestens ein Eingabeelement, mindestens ein Ausgabeelement, einen Prozessor mit einem Speicher und einer Software sowie eine Sende- und Empfangselektronik auf.

Ferner weist das System eine Gegenstation auf, die an bzw. in der Nähe einer Zieleinrichtung angeordnet ist bzw. mit dieser in Wirkverbindung steht. Die Gegenstation weist eine Lese- und Auswerteelektronik zur Überprüfung der Berechtigung des Identmediums, einen Aktor und einen Speicher auf.

Das System weist ferner temporär ein Wechsel B-Feld zum verschlüsselten, drahtlosen bidirektionalen Datenaustausch bzw. zum Durchführen einer sogenannten Challenge Response auf. Das System ist weiterhin derartig ausgebildet, dass es Signale im niederfrequenten Bereich sendet. Identmedium und/oder Gegenstation sind programmierbar, besonders bevorzugt drahtlos programmierbar.

Vorzugsweise weisen Identmedium und/oder Gegenstation eine handliche Größe, beispielsweise die Größe einer Streichholzschachtel auf. Ferner sind Identmedium und/oder Gegenstation vorzugsweise örtlich versorgt bzw. batterieversorgt. Weiterhin weisen das Identmedium und/oder die Gegenstation vorzugsweise eine Batterie- oder Akkuzelle auf und/oder sind direkt aufladbar. Der mindestens eine Biometriesensor ist vorzugsweise als Fingerprintsensor, Iris-, Face-Recognitionsensor etc. ausgebildet und ist weiterhin vorzugsweise mit einer Lebenderkennung, bevorzugt mit einem Pulssensor oder Körpertemperatursensor verbunden.

Der Biometriesensor des Identmediums ist besonders bevorzugt als Fingerprintsensor ausgebildet und arbeitet vorzugsweise optisch, kapazitiv, thermisch oder mit Radiowellen. Vorzugsweise ist der Sensor ein Flächen- oder Streifensensor. Ein Streifensensor, bei dem der Finger über den Sensor bewegt wird, erweist sich gegenüber einem Flächensensor, auf den der Finger aufgelegt wird, dahingehend als vorteilig, dass er eine kleinere Fläche aufweist und somit billiger, platzsparender und weniger Schmutzanfällig ist. Ferner verbleiben auf einem Streifensensor keine remanenten Spuren des Fingers bzw. Fingerabdrucks, die missbraucht werden könnten.

Das Eingabeelement des Identmediums ist vorzugsweise als Taste bzw. Tastenfeld, Schalter, Tastatur und/oder dergleichen ausgebildet. Als Ausgabeelement werden vorzugsweise sichtbare Ausgabeelemente wie beispielsweise LED, Display oder dergleichen, oder hörbare Ausgabeelemente, wie Lautsprecher, Geräusch- bzw. Klangerzeugungseinrichtungen verwendet.

Der drahtlose bidirektionale Datenaustausch zwischen Identmedium und Gegenstation mittels eines Wechsel B-Felds ermöglicht, beispielsweise im Vergleich zu einem rein elektrischen Wechsel E-Feld, einen sicheren Datenaustausch bzw. eine sichere Abarbeitung eines Zutrittskontrollprotokolls bzw. einer Challenge Response im Falle einer räumlichen Trennung von Identmedium und Gegenstation, beispielsweise durch Wände, Türen, Stahl, Metall, Stahlarmierungen, Metallarmierungen und/oder dergleichen. Die Kommunikation über ein Wechsel B-Feld erfolgt vorzugsweise im Längstwellen-, Langwellen oder Mittelwellen-Frequenzbereich. Das Wechsel B-Feld hat vorzugsweise eine Reichweite von bis zu etwa 1,5 m und besonders bevorzugt von etwa bis zu 2,5 m oder mehr. Hieraus ergibt sich insbesondere der Vorteil, dass sich ein versehentliches Öffnen oder Schließen vermieden wird. Vor allem dadurch, dass ein derartiger Vorgang durch den Benutzer aufgrund seiner Nähe zur Zieleinrichtung durch sichtbare oder hörbare Zeichen, bspw. das Schalten einer Schließvorrichtung bzw. das Öffnen einer Tür oder das Starten eines Motors, sofort erkannt und rückgängig gemacht werden kann.

Weiterhin werden Signale zwischen Identmedium und Gegenstation vorzugsweise im niederfrequenten Bereich gesendet. Vorzugsweise erfolgt die Kommunikation bzw. der Datenaustausch zwischen Identmedium und Gegenstation über ein elektromagnetisches Feld, wobei nur die B-Feld-Komponente des elektromagnetischen Feldes nicht aber die E-Feld Komponente genutzt wird.

Während das Identmedium tragbar ausgebildet ist, um von einem Benutzer mitgeführt werden zu können, ist die Gegenstation an bzw. in der Nähe der Zieleinrichtung angeordnet bzw. steht mit dieser in Wirkverbindung. Zieleinrichtungen sind hierbei vorzugsweise Türen, Türzylinder aller Art,

insbesondere Gebäudetüren, Autotüren, Safe- oder Tresortüren, Schaltschranktüren, Möbeltüren sowie weitere Schließelemente und/oder Verriegelungseinrichtungen, die geeignet sind, einen physikalischen Zugang zu einer Zieleinrichtung wie beispielsweise einem Raum, einem Auto, einem Tresor oder einem Geldautomaten zu gewährleisten. Weiterhin werden unter Zieleinrichtungen Systeme wie logische Sperrmechanismen, Computersysteme und/oder schaltungs- oder softwarebasierte Zutritts- bzw. Zugriffskontrollsysteme wie beispielsweise Fahrerberechtigungen oder Zündberechtigungen im Kfz-Bereich, Log-ons zu Computern oder Computersystemen sowie das Freischalten von Schusswaffensicherungssystemen verstanden. Die Zieleinrichtung zeichnet sich demnach dadurch aus, dass ein logischer und/oder physikalischer Zugang zu derselben möglich ist, wobei dieser Zugang bzw. Zugriff erlaubt oder nicht erlaubt bzw. möglich oder nicht möglich ist.

Das erfindungsgemäße System ermöglicht somit beispielsweise das Öffnen und Verschließen sowie das Abschließen oder Verriegeln von Türen bzw. Schließeinrichtungen aller Art oder beispielsweise das Sichern und Entsichern von Schusswaffen. Die Durchführung des Ermöglichen bzw. Verhinderns eines logischen und/oder physikalischen Zugangs zu der Zieleinrichtung wird durch den Aktor vorgenommen. Der Aktor ist vorzugsweise als Magnet bzw. Hubmagnet, Motor, Schaltung, Prozessor, Softwareprogramm und/oder dergleichen ausgebildet. Vorzugsweise steht der Aktor mit einem Sperrelement und/oder einem Kupplungselement in Verbindung und sperrt bzw. entsperrt dieses bzw. entkuppelt dieses oder kuppelt dieses ein. Hierbei erfolgt das Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu der Zieleinrichtung vorzugsweise über das Sperr- und/oder Kupplungselement.

Das Identmedium ist vorzugsweise handlich ausgebildet, so dass es durch den Benutzer bequem mitzuführen ist. Weiterhin ist das Identmedium vorzugsweise als Akkuzelle eines Mobiltelefons ausgebildet oder an bzw. in der Nähe einer solchen angeordnet. In der bevorzugten Ausführungsform des Identmediums als Akku eines Mobiltelefons oder dergleichen ist dieser vorzugsweise zum Aufstecken auf ein Handy (wie beispielsweise bei Nokia Handys 6210) bzw. zum Einlegen in das

Akkufach eines Handys mit zusätzlicher Oberschale (wie bei Handys der Firma Siemens) ausgebildet.

Zum sicheren personalisierten Identifizieren eines Benutzers weist der Prozessor bzw. der Speicher des tragbaren Identmediums vorzugsweise eine dezentrale Datenbank auf. Diese Datenbank ist vorzugsweise für das jeweilige Identmedium spezifisch. Weiterhin weist die Datenbank bevorzugt eingelernte Biometriedaten auf. Somit ermöglicht bereits das tragbare Identmedium ein sicheres personalisiertes Identifizieren eines Benutzers. Die Datenbank ist vorzugsweise derart ausgebildet, dass sie off-line ist, also direkt bzw. ausschließlich über das Identmedium erstellbar und/oder bearbeitbar ist. Weiterhin oder zusätzlich weist das Identmedium vorzugsweise eine Schnittstelle zum Anschluss an bspw. einen PC auf, der zur Bearbeitung der Datenbank verwendbar ist.

Vorzugsweise ist den in der Datenbank abgelegten Daten bzw. benutzerspezifischen Informationen ein Status, beispielsweise eine Hierarchie zugeordnet. Somit lässt sich beispielsweise zwischen Normal-Usern und Super-Usern mit unterschiedlichen Berechtigungen unterscheiden. Die von dem Identmedium gesendeten Daten und Signale weisen vorzugsweise unter anderem Informationen über den Status eines Benutzers (Normal-User/Super-User) auf. Vorzugsweise weisen die Signale weiterhin Informationen über die Berechtigung (berechtigt / beschränkt berechtigt / nicht berechtigt) des jeweiligen Benutzers auf. Vorzugsweise sind die dem Status bzw. der Berechtigung entsprechenden zulässigen und nicht zulässigen Handlungen in der Gegenstation bzw. der Datenbank der Gegenstation abgelegt. Die Gegenstation bzw. die Auswerteelektronik der Gegenstation veranlasst nach Überprüfung der Berechtigung des Identmediums als Reaktion auf die empfangenen Informationen eine entsprechende Aktion. Hierbei ist die Reaktion beispielsweise abhängig von dem Benutzerstatus.

Wie bereits beschrieben, sind Identmedium und Gegenstation vorzugsweise drahtlos programmierbar. Besonders bevorzugt sind Identmedium und/oder

Gegenstation ausschließlich durch mindestens einen entsprechend berechtigten Benutzer, insbesondere ohne Zuhilfenahme weiterer Mittel, programmierbar.

Weitere Merkmale des erfindungsgemäßen Systems bzw. des Identmediums und/oder der Gegenstation ergeben sich aus der folgenden Diskussion eines erfindungsgemäßen Verfahrens, wobei in der folgenden Diskussion des erfindungsgemäßen Verfahrens auf die zuvor beschriebenen System- bzw. Vorrichtungsmerkmale im wesentlichen nicht weiter, es sei denn ergänzend, eingegangen wird.

Das erfindungsgemäße Verfahren zum sicheren personalisierten Identifizieren Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu bzw. Zugriffs auf eine Zieleinrichtung, das vorzugsweise mittels einer beschriebenen Vorrichtung durchgeführt wird, weist die folgenden Schritte auf.

Zunächst erfolgt das Identifizieren eines Benutzers mittels eines tragbaren Identmediums, wobei biometrische Daten mindestens eines Benutzers durch mindestens einen Biometriesensor detektiert werden und wobei Daten und/oder Befehle über mindestens ein Eingabeelement eingegeben und Betriebszustände und/oder Informationen über mindestens ein Ausgabeelement ausgegeben bzw. angezeigt werden.

Mittels eines Prozessors mit einem Speicher und einer Software, welche eine dezentrale, für das Identmedium spezifische, Datenbank mit eingelernten Biometriedaten aufweist, erfolgt ein Vergleich zwischen den detektierten Biometriedaten des mindestens einen Benutzers und den eingelernten Biometriedaten.

Anschließend erfolgt das Senden eines Signals bzw. von Daten im niederfrequenten Bereich über ein Wechsel B-Feld in einem bidirektionalen Datenaustausch bzw. über eine Challenge Response mittels einer Sende- und Empfangselektronik, wobei die Kommunikation mit einer an bzw. in der Nähe der Zieleinrichtung angeordneten bzw. mit dieser in Wirkverbindung stehenden Gegenstation erfolgt. Das Senden von

derartigen Daten, Signalen und/oder Informationen erfolgt ausschließlich nach einer erfolgreichen Identifikation des autorisierten Benutzers. Vorzugsweise erfolgt der obige Schritt im Anschluß an die erfolgreiche Identifkiation eines autorisierten Benutzers automatisch und/oder durch einen entsprechenden Impuls. Ein derartiger Impuls kann beispielsweise durch den Benutzer über das Eingabeelement oder aber durch ein entsprechendes Signal der Gegenstation gegeben werden.

Empfängt die Gegenstation ein Signal des Identmediums, erfolgt die Überprüfung der Berechtigung des Identmediums bzw. des gesendeten Signals mittels einer Lese- und Auswerteelektronik.

Auf die obige Berechtigungsüberprüfung folgt entsprechend dem empfangenen Signal das Ermöglichen oder Verhindern bzw. Zulassen oder nicht Zulassen eines logischen und/oder physikalischen Zugangs zu bzw. Zugriffs auf eine Zieleinrichtung mittels eines Aktors. Die konkrete Handlung richtet sich vorzugsweise nach einer entsprechenden Eingabe des Benutzers oder ist vorgegeben.

Weiterhin erfolgt eine Speicherung eines jeden Vorgangs mit zumindest Datum, Uhrzeit und Kennzeichnung des Identmediums im Identmedium und/oder der Gegenstation.

Identmedium und/oder Gegenstation sind vorzugsweise programmierbar, besonders bevorzugt drahtlos programmierbar bzw. über eine Software programmierbar ausgebildet. Eine derartige Programmierung kann jederzeit vorgenommen werden, wobei vorzugsweise zunächst eine erfolgreiche Identifikation eines Benutzers durch das Identmedium vorausgegangen sein muß.

Weiterhin ist die Datenbank des Identmediums vorzugsweise veränderlich ausgebildet, so dass in weiteren Verfahrensschritten zusätzliche Biometriedaten eingelernt und/oder bearbeitet werden können. Vorzugsweise muß zur Bearbeitung bzw. Veränderung der Datenbank eine erfolgreiche Identifizierung eines entsprechend berechtigten Benutzers vorausgegangen sein.

Hierdurch kann eine einmal erstellte Datenbank, die in einem ersten Schritt eingelernt bzw. generiert wurde, durch einen berechtigten Benutzer, der das Identifikationsverfahren erfolgreich durchlaufen hat, jederzeit neu eingelernt, verändert bzw. gelöscht werden. Hierzu können jeweilige Benutzerdaten, die über das Ausgabeelement angezeigt werden bzw. identifiziert oder zugeordnet werden können, gelöscht werden oder können die Daten eines neuen Benutzers eingelesen werden, wobei hierzu ein Einlesen der Biometriedaten, beispielsweise des Fingerabdrucks, durch den Biometrie- bzw. Fingerprintsensor des Identmediums erfolgt. Vorzugsweise erfolgt eine derartige Bearbeitung der Datenbank ausschließlich mittels des Identmediums, d.h. ohne Verwendung eines PC etc. Weiterhin ist vorzugsweise kein Abgleich mit einer zentralen Datenbank erforderlich. Vorzugsweise kann die Datenbank zusätzlich über eine Schnittstelle durch einen PC bearbeitet oder verändert werden.

Vorzugsweise ist das vom Identmedium ausgesendete Signal bzw. der ausgesendete Code nicht nur abhängig von einer erfolgten positiven Identifizierung sondern auch von einer zugeordneten Berechtigungsebene. Hierbei existiert neben der Unterscheidung berechtigt/nicht berechtigt eine Unterscheidung der Benutzerhierarchie beispielsweise in „Normal-User", „Super-User", etc. Vorzugsweise lassen Identmedium und/oder Gegenstation je nach Hierarchiestufe des identifizierten Benutzers nur definierte Aktionen zu. Beispielsweise sendet hierbei zunächst das Identmedium der Hierarchieebene des identifizierten Benutzers entsprechende Signale bzw. Informationen an die Gegenstation, wobei diese in Abhängigkeit der empfangenen Signale bzw. Daten bestimmte Aktionen zulässt bzw. durchführt.

So kann vorzugsweise das Identmedium und/oder die Gegenstation durch Benutzer einer bestimmten Hierarchieebene für eine definierte Anzahl an beispielsweise Öffnungs- und/oder Schließvorgängen und/oder temporär, beispielsweise über einen Zeitraum von einer Stunde, freigeschaltet werden. Weiterhin kann die Gegenstation, beispielsweise als Fahrerberechtigung eines Kfz, für Benutzer einer bestimmten Hierarchieebene lediglich eine begrenzte Geschwindigkeit etc. ermöglichen. Im Bereich von Zutrittsberechtigungen zu Gebäuden oder

verschiedenen einzelnen Räumen kann beispielsweise lediglich eine Zutrittsberechtigung für einzelne Bereiche bzw. Räume ermöglicht werden.

Weiterhin kann das Identmedium nach und/oder mit erfolgreicher Identifizierung eines entsprechend autorisierten Benutzers vorzugsweise derart eingestellt werden, dass ein dauerhaftes Signal gesendet wird, so dass beispielsweise eine verschlossene Tür automatisch öffnet sobald sich das Identmedium im Kommunikationsradius zur jeweiligen Gegenstation befindet. Eine derartige Funktion kann vorzugsweise automatisch aktiviert werden oder aber durch eine entsprechende Eingabe des berechtigten Benutzers aktiviert werden. Vorzugsweise ist eine derartige Funktion zeitlich beschränkt aktivierbar.

Vorzugsweise lässt sich das Erfordernis einer biometrischen Erkennung vor dem Senden von Daten und Informationen des Identmediums durch einen entsprechend berechtigten Benutzer temporär oder dauerhaft ausschalten. Nach einer einmaligen biometrischen Identfizierung des berechtigten Benutzers sendet das Identmedium Signale dauerhaft und/oder auf entsprechenden Impuls durch den Benutzer und/oder Gegenstation. Zusätzlich und/oder an Stelle zur biometrischen Identifizierung des berechtigten Benutzers ist zur erfolgreichen Identifikation vorzugsweise die korrekte Eingabe einer PIN (personal identification number) oder eines Passworts erforderlich. Das Einlernen, Löschen oder Ändern von Passwörtern, PINs oder dergleichen erfolgt entsprechend der bereits beschriebenen Veränderung bzw. Bearbeitung der im Identifikationsmedium ablegten Datenbank.

Vorzugsweise erfolgt mit jeder Aktion des Identmediums und/oder der Gegenstation eine entsprechende Protokollierung durch das Identmedium und/oder die Gegenstation, wobei ferner oder zusätzlich die Identifikationsversuche und/oder -vorgänge sowie Eingänge und/oder verhinderte bzw. verweigerte Eingänge, Schließvorgänge oder dergleichen protokolliert werden.

Im Folgenden wird die vorliegende Erfindung beispielhaft anhand einer bevorzugten Ausführungsform bzw. einem bevorzugten Verfahren unter Bezugnahme auf die Zeichnungen beschrieben. Hierbei wird lediglich auf die zur beispielhaften

Beschreibung erforderlichen Merkmale eingegangen. Weitere oder zusätzliche Merkmale bzw. Ausführungsformen ergeben sich aus der vorangegangenen Beschreibung.

Es zeigen:

Fig. 1 eine Prinzipdarstellung einer bevorzugten Ausführungsform des Identmediums in der Draufsicht von außen;

Fig. 2 eine Prinzipskizze einer Innenansicht des Identmediums entsprechend Fig. 1; und

Fig. 3 einen bevorzugten Verfahrensablauf der Abfrage zum Auslösen eines Signals in einer bevorzugten Ausführungsform.

Fig. 1 zeigt eine Skizze einer Außenansicht von oben auf eine bevorzugte Ausführungsform des Identmediums 1, aufweisend einen Biometriesensor 2, ein Ausgabeelement 3 sowie ein Eingabeelement 4. Das Identmedium weist vorzugsweise das Format einer Streichholzschachtel, besonders bevorzugt eine Länge von etwa 3 cm bis 6 cm, eine Breite von etwa 2 cm bis 4 cm sowie eine Höhe von etwa 1 cm bis 2,5 cm auf. Das Gehäuse des Identmediums 1 ist vorzugsweise leicht und robust ausgebildet, beispielsweise aus Aluminium und Kunststoff. Der Biometriesensor 2 ist vorzugsweise als Fingerprintsensor ausgebildet, auf den ein Finger bzw. eine Fingerkuppe eines Benutzers zur Identifikation aufgelegt werden muß (beispielsweise Flächensensor) oder über den ein Finger bzw. eine Fingerkuppe zur Identifikation gezogen werden muß (beispielsweise Streifensensor). Das Ausgabeelement 3 ist beispielsweise als LED ausgebildet während das Eingabeelement 4 vorzugsweise als Taster bzw. Tastenelement ausgebildet ist.

Fig. 2 zeigt eine Prinzipskizze der Innensicht des Identmediums entsprechend Fig. 1 mit dem Biometriesensor 2 und dem Ausgabeelement 3. Das Eingabeelement 4 ist in der Darstellung entsprechend Fig. 2 aus Übersichtlichkeitsgründen nicht

dargestellt. Das Identmedium weist vorzugsweise im Inneren eine Energie- bzw. Stromversorgung 5, eine Sende- und Empfangselektronik 6 mit einer Sende- und Empfangsantenne 7 sowie einen Prozessor 8 mit einem Speicher und einer Software auf.

Die Energie- bzw. Stromversorgung 5 des Identmediums ist vorzugsweise als Batterie oder Akkuzelle ausgebildet. Die Sende- und Empfangselektronik 6 mit der Sende- und Empfangsantenne 7 dient insbesondere zum Generieren bzw. Empfangen eines Wechsel B-Felds zum verschlüsselten, bidirektionalen Datenaustausch bzw. zum Durchführen einer Challenge Response und zum Senden von Signalen im niederfrequenten Bereich. Der Prozessor 8 weist vorzugsweise eine Datenbank auf, die bevorzugt über das Identmedium, d.h. über das Eingabeelement 4, dem Biometriesensor 2, vorzugsweise unter Zuhilfenahme des Ausgabeelements 3, erstellbar bzw. einlernbar oder veränderbar ist. Hierbei dient das Ausgabeelement 3 vorzugsweise zur Kommunikation mit dem Benutzer während des Einlernens bzw. des Bearbeitungsprozesses.

Weitere, zusätzliche oder ergänzende Merkmale des Identmediums 1 sowie der Gegenstation (nicht dargestellt) ergeben sich aus der vorangegangenen Beschreibung.

Fig. 3 zeigt einen bevorzugten Verfahrensablauf der Abfrage zum Auslösen eines Signals des Identmediums 1. Hierbei befindet sich das Identmedium 1 zunächst in einem Ruhezustand bzw. Standby-Mode (S1). Durch eine entsprechende Eingabe, beispielsweise durch Tastendruck auf ein als Taster oder Tastatur ausgebildetes Eingabeelement 4 (S2) wird das Identmedium aktiviert bzw. in einen Wachzustand versetzt. Anschließend erfolgt die Identifikation des Benutzers, vorzugsweise durch Auflegen bzw. Überziehen des Fingers auf bzw. über einen als Fingerprintsensor ausgebildeten Biometriesensor 2 (S3). Das Identmedium 1 vergleicht die detektierten Daten bzw. den eingelesenen Fingerabdruck mit in der Datenbank im Prozessor 8 abgelegten Daten bzw. Identifizierungsmerkmalen (S4). Stimmen die eingelesenen Daten nicht mit den abgelegten Daten überein (S5), erwartet das Identmedium ein erneutes Einlesen von Biometriedaten (S3). Stimmen die Daten

jedoch überein (S6), übermittelt der Prozessor 8 ein codiertes Signal an die Sende- und Empfangselektronik 6 zum Starten eines Funkprotokolls (S7). Hierbei erfolgt eine Kommunikation mit einer Gegenstation, vorzugsweise über ein Wechsel B-Feld zum verschlüsselten, bidirektionalen Datenaustausch bzw. zum Durchführen einer Challenge Response. Ist das Funkprotokoll nicht erfolgreich, wechselt das Identmedium vorzugsweise in den Standby-Mode (S8). Ist das Funkprotokoll, beispielsweise die Challenge Response, erfolgreich (S9), erfolgt eine Autorisierung des Zugangs bzw. Zutritts etc., beispielsweise das Öffnen einer Tür zur Zieleinrichtung (nicht dargestellt) über die mit dieser in Verbindung stehende Gegenstation (nicht dargestellt) (S10).

Vorzugsweise wechselt die Vorrichtung, bzw. das Identmedium, sobald nach Überschreiten einer eingestellten Zeitdauer keine Eingabe, beispielsweise S3, erfolgt oder keine weiteren Signale bzw. Eingaben empfangen werden, beispielsweise S8 oder S10, in den Standby-Mode S1. Entsprechend wechselt die Vorrichtung bei S5 vorzugsweise nach erfolgloser n-ter, bevorzugt vierter, Eingabe und/oder nach Ablauf einer bestimmten Zeitdauer ebenfalls in den Standby-Mode S1.

Weitere, zusätzliche oder alternative Merkmale des erfindungsgemäßen Verfahrens entsprechend den vorstehend Beschriebenen.

Das System bzw. das Verfahren gemäß der vorliegenden Erfindung ist dahingehend vorteilhaft, dass es die gestellte Aufgabe(n) erfüllt. Weiterhin ermöglicht die vorliegende Erfindung eine Vielzahl physikalischer und/oder logischer Zugänge für einen Nutzer, wobei dieser lediglich durch einen Biometriesensor identifiziert werden muß. Eine Vielzahl aufwendiger Identifikations- und Zugangskontrollvorrichtungen kann somit entfallen. Hierdurch werden vor allem die Hardware- und Verwaltungskosten, z.B. Einlernkosten, verringert. Neben der Kostenersparnis wirkt sich auch die Verwendungs- bzw. Prozesserleichterung vorteilhaft aus. Ferner können die Vorteile funkbasierter Schließ- und Identifikationsmechanismen, wie beispielsweise Verkabelungsfreiheit, einfache Nachrüstung, Leseeinheit im Innenbereich etc., in vollem Umfang ausgenützt

werden, wodurch sich insbesondere eine hohe Modularität und Wirtschaftlichkeit ergibt. Ferner bietet die vorliegende Erfindung ein sicheres System bzw. Verfahren, da beispielsweise ein verlorenes Identmedium unschädlich ist, da es vom nicht berechtigten Erfinder nicht aktiviert werden kann und somit für diesen wertlos ist. Dennoch ermöglicht das erfindungsgemäße System bzw. Verfahren eine hohe Benutzerfreundlichkeit, da das Identmedium trotz der hohen Sicherheit durch den berechtigten Benutzer übertragbar ist, da dieser in Sekundenschnelle weitere Benutzer einlernen und/oder ihnen Berechtigungen erteilen kann. Hierbei muß der Besitzer lediglich beispielsweise die biometrischen Daten weiterer Personen in das Identmedium einlesen. Eine aufwendige Programmierung einer oder mehrerer Gegenstationen ist somit nicht erforderlich. Auch kann ein derartiges Einlernen unabhängig vom Standort erfolgen, das heißt ein Kontakt zur Zieleinrichtung oder zur Gegenstation ist nicht erforderlich.

SimonsVoss Technologies AG
u.Z.: H 2554 DE

08. September 2003

PATENTANSPRÜCHE

1. System zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu einer Zieleinrichtung, aufweisend
ein tragbares Identmedium mit
mindestens einem Biometriesensor,
mindestens einem Eingabeelement und mindestens einem Ausgabeelement,
einem Prozessor mit einem Speicher und einer Software
sowie einer Sende- und Empfangselektronik und
eine Gegenstation, die an der Zieleinrichtung angeordnet ist bzw. mit dieser in Wirkverbindung steht, mit
einer Lese- und Auswerteelektronik zur Überprüfung der Berechtigung des Identmediums,
einem Aktor und
einem Speicher, wobei
ein Wechsel B-Feld zum verschlüsselten, bidirektionalen Datenaustausch bzw. zum Durchführen einer Challenge Response generiert wird, Signale im niederfrequenten Bereich gesendet werden und wobei Identmedium und/oder Gegenstation programmierbar sind.

2. Vorrichtung nach Anspruch 1, wobei der Biometriesensor als Fingerprintsensor ausgebildet ist.

3. Vorrichtung nach Anspruch 1 oder 2, wobei der Sensor ein optischer, kapazitiver, thermischer oder mit Radiowellen arbeitender Sensor ist.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, wobei der Sensor ein Flächen- oder Streifensensor ist.

5. Vorrichtung nach einem der vorstehenden Ansprüche, wobei das Eingabeelement als Taster oder Tastatur ausgebildet ist.

6. Vorrichtung nach einem der vorstehenden Ansprüche, wobei das Ausgabeelement als LED und/oder als Display ausgebildet ist.

7. Vorrichtung nach einem der vorstehenden Ansprüche, wobei die Vorrichtung dergestalt ist, dass das Wechsel B-Feld eine Reichweite von bis zu 2,5 m hat.

8. Vorrichtung nach einem der vorstehenden Ansprüche, wobei die Vorrichtung dergestalt ist, dass das Wechsel B-Feld durch Wände, Türen, Tresore sowie Stahl, Metall, Armierungen und dergleichen dringen kann.

9. Vorrichtung nach einem der vorstehenden Ansprüche, wobei der Aktor ein Hubmagnet, Motor, Prozessor, Softwareprogramm oder dergleichen aufweist.

10. Vorrichtung nach einem der vorstehenden Ansprüche, wobei der Aktor mit einem Sperrelement oder einem Kupplungselement in Wirkverbindung steht und dieses freigibt bzw. einkuppelt.

11. Vorrichtung nach einem der vorstehenden Ansprüche, wobei das Identmedium als Akkuzelle eines Mobiltelefons ausgebildet ist.

12. Vorrichtung nach einem der vorstehenden Ansprüche, wobei das System eine Batterie oder Akkuzelle aufweist und/oder direkt aufladbar ist.

13. Vorrichtung nach einem der vorstehenden Ansprüche, wobei Identmedium und Gegenstation drahtlos programmierbar sind.

14. Vorrichtung nach einem der vorstehenden Ansprüche, wobei Identmedium und/oder Gegenstation örtlich versorgt bzw. batterieversorgt sind.

15. Vorrichtung nach einem der vorstehenden Ansprüche, wobei der Prozessor des Identmediums eine dezentrale, für das Identmedium spezifische, Datenbank mit eingelernten Biometriedaten aufweist.

16. Vorrichtung nach Anspruch 15, wobei die Datenbank über das Identmedium veränderbar ist.

17. Verfahren zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu einer Zieleinrichtung, aufweisend die Schritte

Identifizieren eines Benutzers mittels eines tragbaren Identmediums, wobei biometrische Daten mindestens eines Benutzers durch mindestens einen Biometriesensor detektiert werden und

Daten und/oder Befehle über mindestens ein Eingabeelement eingegeben und Betriebszustände über mindestens ein Ausgabeelement angezeigt werden, und wobei mittels eines Prozessors mit einem Speicher und einer Software, welcher eine dezentrale, für das Identmedium spezifische, Datenbank mit eingelernten Biometriedaten aufweist, ein Vergleich zwischen den detektierten Biometriedaten und den eingelernten Biometriedaten durchgeführt wird;

Senden eines Signals im niederfrequenten Bereich über ein Wechsel B-Feld in einem bidirektionalen Datenaustauschs bzw. über eine Challenge Response mittels einer Sende- und Empfangselektronik nach erfolgreichem Identifizieren eines autorisierten Benutzers an eine an einer Zielstation angeordnete oder mit dieser in Wirkverbindung stehende Gegenstation,

Überprüfen der Berechtigung des Identmediums bzw. des gesendeten Signals mittels einer Lese- und Auswerteelektronik durch die Gegenstation;

Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs bzw. Zutritts zu einer Zieleinrichtung mittels eines Aktors; und

Speichern eines jeden Vorgangs mit Datum, Uhrzeit, Kennzeichnung des Identmediums und/oder des Benutzers.

18. Verfahren nach Anspruch 17, wobei Identmedium und/oder Gegenstation programmierbar sind.

19. Verfahren nach Anspruch 18, wobei Identmedium und/oder Gegenstation drahtlos programmierbar sind.

20. Verfahren nach einem der Ansprüche 17 bis 19, wobei die Datenbank über das Identmedium bearbeitbar bzw. veränderbar ist, indem weitere Biometriedaten eingelernt, gelöscht und/oder bearbeitet werden.

21. Verfahren nach Anspruch 20, wobei die Bearbeitung der Datenbank off-line, d.h. direkt über das Identmedium, erfolgt.

22. Verfahren nach einem der Ansprüche 17 bis 21, wobei die Detektion von Biometriedaten mittels eines Fingerprintsensors erfolgt, der Fingerabdrücke nach einem optischen oder kapazitiven Verfahren detektiert.

23. Verfahren nach einem der Ansprüche 17 bis 22, wobei der Sensor optisch, kapazitiv, thermisch oder mit Radiowellen arbeitet.

24. Verfahren nach einem der Ansprüche 17 bis 23, wobei die Eingabe mittels eins Tasters oder einer Tastatur erfolgt.

25. Verfahren nach einem der Ansprüche 17 bis 24, wobei die Ausgabe mittels einer LED und/oder eines Displays erfolgt.

26. Verfahren nach einem der Ansprüche 17 bis 25, wobei der Aktor ein Hubmagnet, Motor, Prozessor, Softwareprogramm oder dergleichen ist.

27. Verfahren nach einem der Ansprüche 17 bis 26, wobei die Biometrische Erkennung durch den berechtigten ausschaltbar ist.

28. Verfahren nach einem der Ansprüche 17 bis 27, wobei nicht nur zwischen berechtigten und unberechtigten Benutzern, sonder ferner zwischen Benutzern mit verschiedenen Berechtigungen bzw. verschiedenen Berechtigungshierarchien unterschieden wird.

29. Verfahren nach Anspruch 28, wobei die Reaktion der Gegenstation von der Berechtigung bzw. der Hierarchie des Benutzers abhängig ist.

30. Verfahren nach einem der Ansprüche 17 bis 29, wobei die Identifikationsversuche und/oder –vorgänge sowie Eingänge und/oder verhinderte bzw. verweigerte Eingänge durch mindestens einen der Prozessoren protokolliert werden.

31. Verfahren nach einem der Ansprüche 17 bis 30, wobei das Identmedium und/oder die Gegenstation örtlich versorgt bzw. batterieversorgt sind.

32. Verfahren nach einem der Ansprüche 17 bis 31, wobei zur Identifikation weiterhin die korrekte Eingabe einer PIN erforderlich ist.

33. Verfahren nach einem der Ansprüche 17 bis 32, wobei die in der Datenbank eingelernten benutzerspezifischen Daten einer Hierarchie zugeordnet sind, wobei Identmedium und/oder Gegenstation je nach Hierarchiestufe des Identifizierten Benutzers nur definierte Aktionen zulassen.

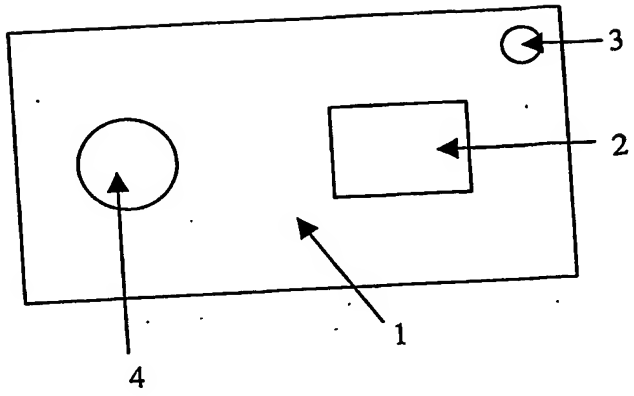

Fig. 1

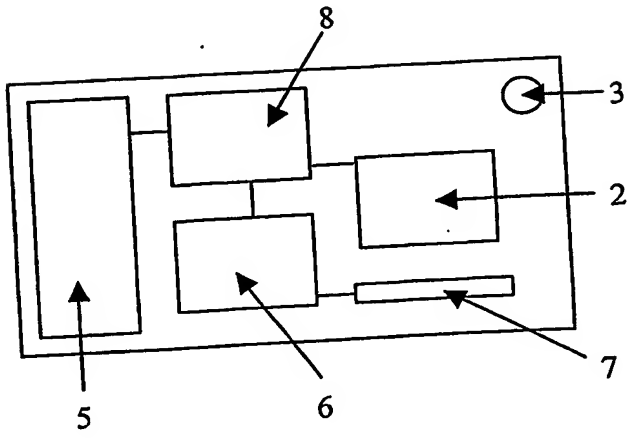

Fig. 2

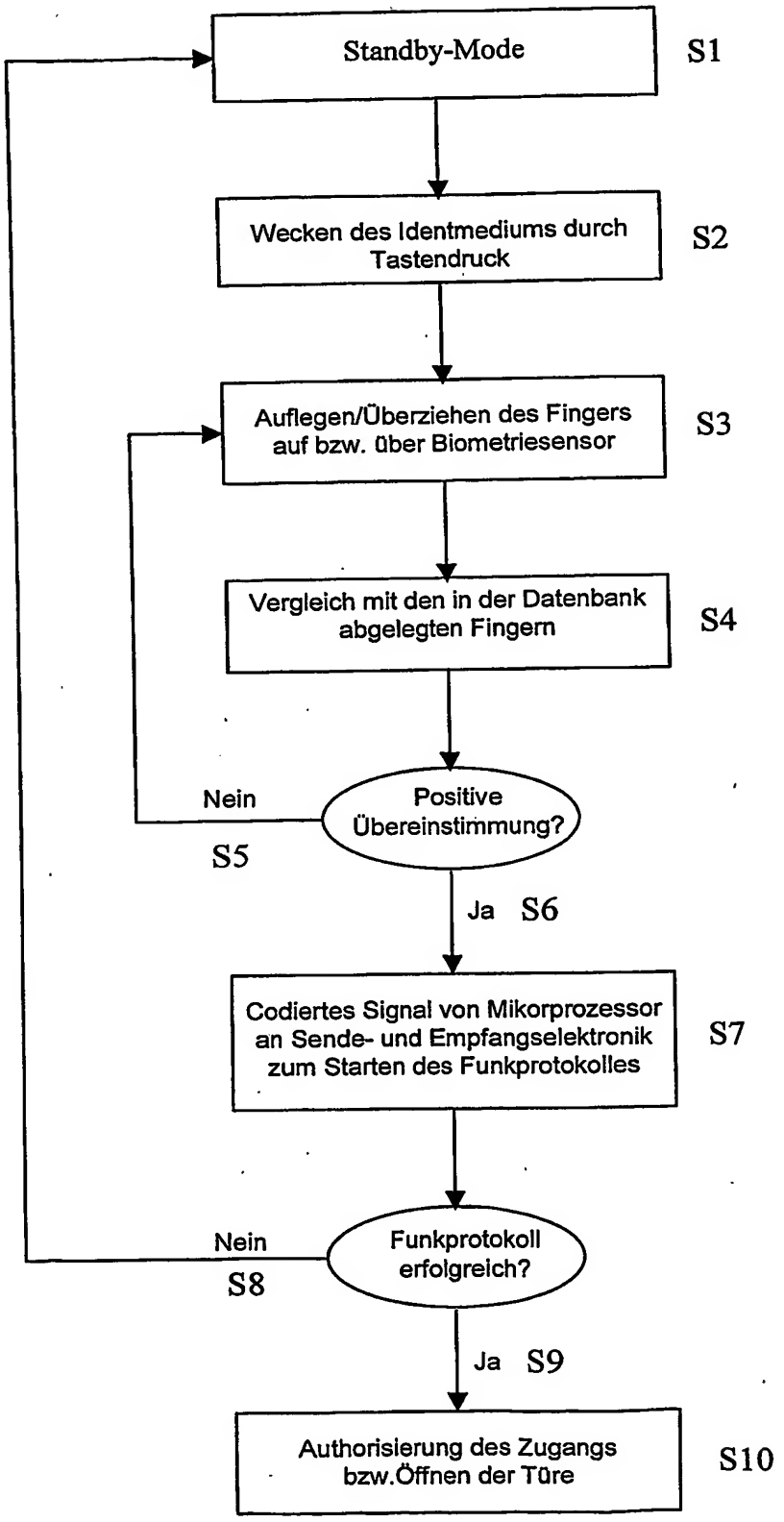
Standby-Mode
S1
Wecken des Identmediums durch Tastendruck
S2
Auflegen/Überziehen des Fingers auf bzw. über Biometriesensor
S3
Vergleich mit den in der Datenbank abgelegten Fingern
S4
Positive Übereinstimmung?
Nein
S5
Ja
S6
Codiertes Signal von Mikorprozessor an Sende- und Empfangselektronik zum Starten des Funkprotokolles
S7
Funkprotokoll erfolgreich?
Nein
S8
Ja
S9
Authorisierung des Zugangs bzw.Öffnen der Türe
S10

Fig. 3

SimonsVoss Technologies AG
u.Z.: H 2554 DE

08. September 2003

ZUSAMMENFASSUNG

Die vorliegende Erfindung betrifft ein System und ein Verfahren zum sicheren personalisierten Identifizieren und Ermöglichen bzw. Verhindern eines logischen und/oder physikalischen Zugangs zu einer Zieleinrichtung. Hierbei weist das System ein ein tragbares Identmedium mit mindestens einem Biometriesensor, mindestens einem Eingabeelement und mindestens einem Ausgabeelement, einem Prozessor mit einem Speicher und einer Software sowie einer Sende- und Empfangselektronik und eine Gegenstation, die an der Zieleinrichtung angeordnet ist bzw. mit dieser in Wirkverbindung steht, mit einer Lese- und Auswerteelektronik zur Überprüfung der Berechtigung des Identmediums, einem Aktor und einem Speicher, wobei ein Wechsel B-Feld zum verschlüsselten, bidirektionalen Datenaustausch bzw. zum Durchführen einer Challenge Response generiert wird, Signale im niederfrequenten Bereich gesendet werden und wobei Identmedium und/oder Gegenstation programmierbar sind.